AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method comprising:

implementing a multi-party secure computation protocol between a client which has a client secret and a server which has a server secret to compute a third secret from the client secret and the server secret, wherein the protocol is implemented so that the client obtains the third secret and cannot feasibly determine the server secret, and the server cannot feasibly determine the client secret [[or]] and cannot feasibly determine the third secret;

authenticating the client by a device, the device storing an encrypted secret and configured not to provide the encrypted secret without authentication; and

after authenticating, providing to the client by the device the encrypted secret, wherein the encrypted secret is capable of being decrypted using a decryption key derived from the third secret and wherein the multi-party secure computation protocol implemented between the client and the server is the only multi-party computation protocol that is implemented in generating the third secret and the decryption key derived from the third secret.

2. (Previously Presented) The method of claim 43 wherein the third secret is derived from the intermediate data by use of one of a key derivation function and a hash function.

3. (Canceled)

4. (Original) The method of claim 1 wherein the client secret comprises at least one of a PIN, a password, and biometric information.

5. (Previously Presented) The method of claim 43 wherein the intermediate data is derived from at least the client secret and the server secret by use of a blind function evaluation protocol.

6. (Original) The method of claim 5 wherein the security of the blind function evaluation protocol is based on the problem of extracting roots modulo a composite.

7. (Original) The method of claim 5 wherein the security of the blind function evaluation protocol uses discrete logarithms.

8. (Previously Presented) The method of claim 1 wherein authenticating comprises authenticating the client based on a time-dependent code.

9. (Previously Presented) The method of claim 1 wherein authenticating comprises authenticating the client based on at least one of a PIN, a password, and biometric information.

10. (Previously Presented) The method of claim 1 wherein authenticating comprises authenticating the client based on a secret other than the client secret.

11. (Previously Presented) The method of claim 1 wherein authenticating comprises using an authentication secret derived from the third secret.

12. (Original) The method of claim 1 wherein the device comprises at least one of a file server, a directory server, a key server, a PDA, a mobile telephone, a smart card, and a desktop computer.

13. (Original) The method of claim 12 wherein the device comprises at least one secure data store, the device requiring authentication before allowing the client access to the data store.

14. (Previously Presented) The method of claim 1 wherein the encrypted secret comprises an encrypted private key of a public/private key pair used for asymmetric cryptography.

15. (Previously Presented) The method of claim 14 wherein the encrypted secret comprises an encrypted signature key used for creating a digital signature.

16. (Previously Presented) The method of claim 15 wherein authenticating comprises authenticating the client based on a secret other than the client secret, so that the user provides different information to access the device and access the signature key.

17. (Previously Presented) The method of claim 1 wherein the encrypted secret comprises an encrypted secret key used for symmetric cryptography.

18. (Previously Presented) The method of claim 1 wherein the encrypted secret comprises at least one unit of encrypted digital currency.

19. (Previously Presented) The method of claim 43 further comprising verifying that the client has not exceeded a predetermined number of unsuccessful attempts to obtain the intermediate data.

20. (Previously Presented) The method of claim 19 wherein verifying further comprises:

transmitting a challenge code to the client; and

receiving the result of a cryptographic operation using the challenge code as an input and using a cryptographic key derived from the encrypted secret.

Claims 21-30. (Canceled)

31. (Previously Presented) The method of claim 1, further comprising

deriving the decryption key from the third secret; and

decrypting the encrypted secret using the decryption key.

Claims 32-37. (Canceled)

38. (Currently Amended) A method for authenticating to a network server, the method comprising:

implementing a multi-party secure computation protocol between a client which has a client secret and a server which has a server secret to compute a third secret from the client secret and the server secret, wherein the protocol is implemented so that the client cannot feasibly determine the server secret and the server cannot feasibly determine the client secret [[or]] and cannot feasibly determine the third secret;

at the client deriving a password from the third secret;

authenticating to the network server using the derived password, wherein the multi-party secure computation protocol implemented between the client and the server is the only multi-party computation protocol that is implemented in generating the third secret and the password derived from the third secret.

39. (Previously Presented) The method of claim 38 further comprising transmitting to the first server by the network server verification that the user has authenticated successfully.

40. (Original) The method of claim 38 wherein the network server is a web server.

41. (Previously Presented) The method of claim 38 wherein deriving comprises deriving a server password using a key derivation function.

42. (Canceled)

43. (Previously Presented) The method of claim 1, wherein implementing the multi-party secure computation protocol involves:

at the client, using the client secret to compute client information and then sending the client information to the server;

at the server, using the client information and the server secret to compute intermediate data and sending the intermediate data to the client; and

at the client, deriving the third secret from the intermediate data.

44. (Previously Presented) The method of claim 1, wherein the multi-party secure computation protocol is a blind function evaluation protocol.

45. (Previously Presented) The method of claim 44, wherein the blind function evaluation protocol is based on discrete-logarithm cryptography.

46. (Previously Presented) The method of claim 45, wherein the blind function evaluation protocol is based on an RSA algorithm.

47. (Currently Amended) A method comprising:

implementing a multi-party secure computation protocol between a client which has a client secret and a server which has a server secret to compute a third secret from the client secret and the server secret, wherein the protocol is implemented so that the client cannot feasibly determine the server secret and the server cannot feasibly determine the client secret [[or]] and cannot feasibly determine the third secret;

authenticating the client by a device, the device storing an encrypted secret and configured not to provide the encrypted secret without authentication; and

after authenticating, providing to the client by the device the encrypted secret, wherein the encrypted secret is capable of being decrypted using a decryption key derived from the third secret and wherein no additional multi-party secure computation protocol involving any entity other than the server is required to enable the client to generate the third secret and the key derived from the third secret.

48. (Previously Presented) The method of claim 38, wherein the password is derived from the third secret and a server identifier.